A NEW ALGORITHM
FOR CONSTRUCTING LARGE CARMICHAEL NUMBERS

GÜNTER LÖH AND WOLFGANG NIEBUHR

ABSTRACT. We describe an algorithm for constructing Carmichael numbers N with a large number of prime factors $p_1, p_2, \ldots, p_k$. This algorithm starts with a given number $\Lambda = \mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$, representing the value of the Carmichael function $\lambda(N)$. We found Carmichael numbers with up to 1101518 factors.

1. INTRODUCTION

A commonly used method to decide whether a given number N is composite is the following easily practicable test: Take some number a with $\gcd(a, N) = 1$ and compute $b \leftarrow a^{N-1} \bmod N$. If $b \neq 1$, our N is composite. Unfortunately, if we get $b = 1$ we cannot be sure that N is prime, even though this is true in many cases. A composite number N which yields $b = 1$ is called a pseudoprime to the base a. If some N yields $b = 1$ for all bases a with $\gcd(a, N) = 1$, this N is called an *absolute pseudoprime* or a *Carmichael number*. These numbers were first described by Robert D. Carmichael in 1910 [3]. The term Carmichael number was introduced by Beeger [2] in 1950. The smallest number of this kind is $N = 3 \cdot 11 \cdot 17 = 561$.

Studying the properties of absolute pseudoprimes, Carmichael defined a function $\lambda(N)$ as follows:

$$\lambda(2^h) = \varphi(2^h) \qquad \text{for } h = 0, 1, 2,$$

$$\lambda(2^h) = \frac{1}{2}\varphi(2^h) \qquad \text{for } h > 2,$$

$$\lambda(q^h) = \varphi(q^h) \qquad \text{for primes } q > 2,$$

$$\lambda(q_1^{h_1} q_2^{h_2} \cdots q_r^{h_r}) = \mathrm{lcm}(\lambda(q_1^{h_1}), \lambda(q_2^{h_2}), \ldots, \lambda(q_r^{h_r})) \quad \text{for distinct primes } q_j,$$

where φ denotes Euler's totient function. Other authors later called the function $\lambda(N)$ the *Carmichael function*. Carmichael [3] showed that N is an absolute pseudoprime if and only if

$$(1) \qquad\qquad N \equiv 1 \pmod{\lambda(N)}.$$

He also showed that absolute pseudoprimes are a product of k distinct odd primes p_k, $k \geq 3$. Later we will use the following properties of Carmichael numbers:

(a) For Carmichael numbers $N = p_1 p_2 \cdots p_k$ the value of the Carmichael function is $\lambda(N) = \operatorname{lcm}(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$.

(b) Let N be a Carmichael number with $\lambda(N) = \Lambda$. If $p = \Lambda + 1$ is prime and $N \not\equiv 0 \pmod{p}$, then Np is also a Carmichael number. (This is a special case of Chernick's Theorem 4, [5].)

(c) There are no natural numbers n, q such that q and $nq + 1$ are both prime factors of a Carmichael number N (see Yorinaga [25]).

In his first paper on this subject [3], published in 1910, Carmichael presented four absolute pseudoprimes including the well-known example $3 \cdot 11 \cdot 17$. The others are $5 \cdot 13 \cdot 17$, $7 \cdot 13 \cdot 31$, and $7 \cdot 31 \cdot 73$. Two years later, he mentioned 11 more absolute pseudoprimes with three factors, and he also found one with four factors, which is $13 \cdot 37 \cdot 73 \cdot 457$ [4]. A larger quantity of absolute pseudoprimes was first determined by Poulet [18] in 1938.

Chernick [5] made some essential contributions to the theory of Carmichael numbers. In 1939, he introduced the universal form

$$U_k(m) = (6m + 1)(12m + 1) \prod_{i=1}^{k-2} (9 \cdot 2^i m + 1)$$

which generates Carmichael numbers if all its factors are prime. Also, he constructed Carmichael numbers with up to seven factors.

Carmichael numbers with a large number of prime factors were investigated in particular by Yorinaga. In 1978 he gave many examples with up to 15 factors [25], and two years later in [26] he published a long table of Carmichael numbers with a number of factors in the range from 13 up to 18, culminating in

$$N_1 = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 73 \cdot 79 \cdot 89 \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 131 \cdot 1783,$$
$$N_2 = 19 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 89 \cdot 101 \cdot 103 \cdot 113 \cdot 127 \cdot 131 \cdot 137 \cdot 4421.$$

Recently a new interest in large Carmichael numbers has arisen. By systematic search, Pinch [16] found

$$N = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 97 \cdot 101 \cdot 109 \cdot 113 \cdot 151 \cdot 181 \cdot 193 \cdot 641,$$

which is the smallest Carmichael number with 20 factors. Zhang found a Carmichael number with 1305 factors [27]. Guillaume and Morain found several Carmichael numbers, the largest one built from 5104 factors [9]. Furthermore, Pinch tabulated all Carmichael numbers up to 10^{16} [17]. In [16], a survey of other efforts to count Carmichael numbers is given.

Simultaneously to the work of Yorinaga, other authors tried to construct Carmichael numbers with many decimal digits using only a few large prime factors. In 1979, Hill found a Carmichael number with three factors and 77 digits [11]. In 1980, Wagstaff published a Carmichael number with 101 digits of type $U_6(m)$ and another one with 321 digits of type $U_3(m)$ [23]. To the latter, Woods and Huenemann successfully added one more prime factor obtaining a new Carmichael number with four factors and 432 digits [24]. In 1989, Dubner [6] published a 1057-digit number of type $U_3(m)$ found in 1985. Furthermore, he described an improved method

for constructing large Carmichael numbers with three prime factors. Using this method he found a 3071-digit number in 1988.

As we have seen, the construction of large Carmichael numbers is often based on the universal form $U_k(m)$ introduced by Chernick. The numbers so constructed have only a few but large prime factors. The difficulty in using this form to produce Carmichael numbers with a large number k of prime factors is the fact that k mutually dependent numbers $(6m+1)$, $(12m+1)$, $(9 \cdot 2^1 m+1)$, ..., $(9 \cdot 2^{k-2} m+1)$ must be prime simultaneously. This problem also occurs in some similar situations, see [19] for primes in arithmetic progressions, [14] for prime chains, and [22, Chapter 3] for prime constellations. In no case could more than 22 of such interrelated primes be determined. Inspecting the approaches suggested in all these situations, we found the use of universal forms to be of no avail in constructing Carmichael numbers with substantially more prime factors. Therefore we initiated the development of a new method.

2. The general algorithm

In order to construct a Carmichael number N, we start with a given value Λ and assume $\Lambda = \lambda(N)$. We then generate all possible prime factors of N according to the properties (a) and (c). This approach is similar to that proposed by Erdős in [7]. Let $\mathcal{S}$ denote the set of all these possible factors, and let κ be the number of elements of $\mathcal{S}$. We compute the product modulo Λ of all primes in $\mathcal{S}$ and call it s. If s equals 1, the product of all primes in $\mathcal{S}$ will constitute a Carmichael number because of (1), but usually s takes some other value. In this case we try to find a small subset $\mathcal{T}$ of primes in $\mathcal{S}$ whose product modulo Λ also equals s. If we discard this subset from $\mathcal{S}$, the remaining primes will constitute a Carmichael number with $k = \kappa - \#\mathcal{T}$ factors. This idea leads to

Algorithm C
  C1 [Start]. Choose an appropriate product of prime powers $\Lambda \leftarrow q_1^{h_1} q_2^{h_2} \ldots q_r^{h_r}$ (with $q_1 = 2$ and $h_j > 0$ for all j).
  C2 [Combine q_j]. Build all

$$p(\alpha_1, \alpha_2, \ldots, \alpha_r) \leftarrow 2^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r} + 1$$

with $1 \le \alpha_1 \le h_1$ and $0 \le \alpha_j \le h_j$ for $j > 1$.
  C3 [Collect admissible factors]. Put all $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$, if they are prime and different from every q_j, $j = 2, 3, \ldots, r$, into the set $\mathcal{S}$. If $\Lambda + 1 \in \mathcal{S}$, set $\mathcal{S} \leftarrow \mathcal{S} \smallsetminus \{\Lambda + 1\}$. [In this case, every Carmichael number with $\lambda(N) = \Lambda$ found by the algorithm can be multiplied by $\Lambda+1$ to give another Carmichael number, see property (b).] Build $s \leftarrow (\prod_{p \in \mathcal{S}} p) \bmod \Lambda$. If $s = 1$, set $\mathcal{T} \leftarrow \varnothing$ and continue with C5.
  C4 [Find $\mathcal{T}$]. Find a set $\mathcal{T} \subset \mathcal{S}$ with $\prod_{p \in \mathcal{T}} p \equiv s \pmod{\Lambda}$.
  C5 [Construct Carmichael number]. Now

$$N = \prod_{p \in \mathcal{S} \smallsetminus \mathcal{T}} p$$

is a Carmichael number.

Remarks. The algorithm does not always guarantee $\lambda(N) = \Lambda$, but only $\lambda(N) \mid \Lambda$. Since $N \equiv 1 \pmod{\Lambda}$ by construction, we also have $N \equiv 1 \pmod{\lambda(N)}$, and N is still a Carmichael number even if $\lambda(N) \neq \Lambda$. However, it should be noted that $\lambda(N) \neq \Lambda$ occurs only in some rare cases where $\#\mathcal{S}$ is small or $\#\mathcal{T}$ is large.

In order to find Carmichael numbers with many prime factors, we try to choose the prime powers $q_j^{h_j}$ in step C1 in a way that we get a large $\kappa = \#\mathcal{S}$ in step C3. It seems reasonable to strive for a large number of $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ in order to have good prospects of obtaining many primes in step C3. The number of $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ built in step C2 is called $H(\Lambda)$. This number equals $h_1 \prod_{j=2}^{r}(h_j + 1)$, and for a given order of magnitude for Λ it becomes large if Λ is a product of suitable powers of small primes. On the other hand, we should try to keep Λ small so that the numbers $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ are small, too. This makes it easier to perform the primality proofs needed in step C3.

We may use so-called *highly composite numbers* n, which were first investigated by Ramanujan [20] in 1915. With respect to their size, these numbers have extraordinarily many divisors, and therefore $H(n)$ is large. The last highly composite number given in a table by Ramanujan yields $H(n) = 8640$ and $\kappa = 2339$. Instead of extending this table we start with a given Λ and try to modify some exponents h_j in order to increase $H(\Lambda)$ without increasing Λ too much.

If we proceed in this way we get many of the same primes within the accompanying sets $\mathcal{S}$. So we may use primes taken from a previous set $\mathcal{S}$ produced by a Λ already treated when dealing with a new large Λ, therefore avoiding repetition of the primality proofs. We did not implement this because it would have involved an inordinate amount of administrative work. Especially for large Λ, step C3 becomes the most time-consuming part of the general algorithm. Since for each $p \in \mathcal{S}$ the factorization of $p - 1$ is known by construction, we used primitive roots for the primality proofs [12, p. 375, p. 395, 609 (exercise 10), p. 397, 614 (exercise 26)].

An approximation of κ. The number κ of elements in $\mathcal{S}$ is an upper bound for the number k of factors of the Carmichael number to be constructed. It would be desirable to know a priori how many of the $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ will be prime in step C3.

In order to develop an approximation $K(\Lambda) \approx \kappa$, we proceed as follows: The probability of a randomly chosen natural number n to be prime is about $1/\log n$ (see, e.g., [8, p. 111]). We look at $H(\Lambda)$ numbers of the kind $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$. For each number $p(\alpha_1, \alpha_2, \ldots, \alpha_r) - 1 < \sqrt{2\Lambda}$ there is exactly one corresponding number $p(h_1 - \alpha_1 + 1, h_2 - \alpha_2, \ldots, h_r - \alpha_r) - 1 > \sqrt{2\Lambda}$ and vice versa. The product of both these numbers is equal to 2Λ. We therefore assume the average size of the numbers $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ to be $\sqrt{2\Lambda}$. Assuming these numbers are indeed chosen randomly, about

$$(2) \qquad\qquad H(\Lambda)/\log \sqrt{2\Lambda}$$

of them would be prime.

However, owing to our special construction of the $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ in step C2, the remainders modulo any prime q_j are not uniformly distributed, and we can expect more primes than predicted by (2). To take into account the actual distribution of

the remainders modulo q_j we multiply (2) by a correction factor and define

$$(3) \qquad K(\Lambda) = \left\lfloor \frac{H(\Lambda)}{\log \sqrt{2\Lambda}} \cdot 2 \prod_{j=2}^{r} \frac{1 - \frac{1}{(q_j-1)(h_j+1)}}{1 - \frac{1}{q_j}} \right\rfloor.$$

The correction factor can be obtained by considerations similar to those used by Hardy and Wright studying the distribution of twin primes [10, pp. 371–373]. For every q_j, $j = 2, 3, \ldots, r$, we have $p(\alpha_1, \alpha_2, \ldots, \alpha_r) = 2^{\alpha_1} q_2^{\alpha_2} \cdots q_j^{\alpha_j} \cdots q_r^{\alpha_r} + 1 \equiv 1 \pmod{q_j}$ if and only if $1 \leq \alpha_j \leq h_j$. The remainder 1 therefore has the probability $h_j/(h_j + 1)$ to occur. The other $q_j - 1$ remainders modulo q_j are uniformly distributed and have the probability $1/(h_j + 1)$ altogether. Each of these has the probability $1/((q_j - 1)(h_j + 1))$, especially the remainder zero. This leads to the probability $1 - 1/((q_j-1)(h_j+1))$ instead of $1 - 1/q_j$ for q_j to divide $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$. For $j = 1$, that is $q_1 = 2$, we get an additional factor of 2 since all $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ are odd by construction.

Equation (3) can also be written as

$$(4) \qquad K(\Lambda) = \left\lfloor \frac{\Lambda}{\varphi(\Lambda) \log \sqrt{2\Lambda}} \prod_{j=1}^{r} \left(h_j + \frac{q_j - 2}{q_j - 1} \right) \right\rfloor.$$

We used approximation (4) to select appropriate values of Λ as input for our algorithm. For sufficiently large Λ, the observed relative error was always below 3%.

Continuing the algorithm. In practice we will not terminate the algorithm after having found a single $\mathcal{T}$ in step C4. It turns out to be fairly easy to get more suitable sets $\mathcal{T}$ at virtually no additional effort. The details of this continuation depend on the implementation of step C4 and will be discussed in §3.

Example. In step C1 we choose the highly composite number $\Lambda = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. With this we combine a total of $4 \cdot 3 \cdot 2 \cdot 2 = 48$ values $p(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ in step C2. According to (4) we expect $K(\Lambda) = 30$ in step C3, and we construct the set

$$(5) \qquad \begin{aligned} \mathcal{S} = \{ &11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71, 73, 113, \\ &127, 181, 211, 241, 281, 337, 421, 631, 1009, 2521 \} \end{aligned}$$

with $\kappa = \#\mathcal{S} = 23$ elements. We compute $s \leftarrow (\prod_{p \in \mathcal{S}} p) \bmod \Lambda = 929$. Now there is a total of $\sum_{\rho=0}^{20} \binom{23}{\rho} = 8388331$ ways to choose a set $\mathcal{T}$ in step C4, and $\varphi(\Lambda) = 1152$ different values of $(\prod_{p \in \mathcal{T}} p) \bmod \Lambda$ can occur. So there is a good chance to find a $\mathcal{T}$ in step C4. Later on we will take up this example again.

3. How to find $\mathcal{T}$

Step C4 can be performed by various methods. We observe that there are at most $\varphi(\Lambda)$ different values of $(\prod_{p \in \mathcal{T}} p) \bmod \Lambda$. Assuming these remainders to be uniformly distributed, the probability for $\prod_{p \in \mathcal{T}} p \equiv a \pmod{\Lambda}$ will be $1/\varphi(\Lambda)$. On the other hand, there is a total of $\sum_{\rho=0}^{\kappa-3} \binom{\kappa}{\rho}$ possibilities to pick a subset $\mathcal{T} \subset \mathcal{S}$.

So, when we check all possible sets $\mathcal{T}$, we expect about $E_{\text{tot}}(\Lambda) = \left(\sum_{\rho=0}^{\kappa-3} \binom{\kappa}{\rho}\right)/\varphi(\Lambda)$ Carmichael numbers; usually there are plenty.

The simplest way to find a suitable set $\mathcal{T}$ is to look for a random set $\mathcal{T} \subset \mathcal{S}$ and check whether $\prod_{p \in \mathcal{T}} p \equiv s \pmod{\Lambda}$. A more deterministic method tests all subsets $\mathcal{T} \subset \mathcal{S}$. Owing to the large number of possible sets $\mathcal{T}$, which cannot all be checked, we first choose a fixed $\rho \leq \kappa - 3$ and then test only the sets with $\#\mathcal{T} = \rho$. In order to reduce the amount of guesswork, for any selected set $\mathcal{T}' \subset \mathcal{S}$ we calculate $u \leftarrow (s/\prod_{p \in \mathcal{T}'} p) \bmod \Lambda$. If $u \in \mathcal{S}$, we set $\mathcal{T} \leftarrow \mathcal{T}' \cup \{u\}$. For implementations of such algorithms see Guillaume and Morain [9]. We can do even better if we build pairs $(u, v) \in \mathcal{S} \times \mathcal{S}$ and then check if there is a corresponding pair $(u', v') \in \mathcal{S} \times \mathcal{S}$ with $u'v' \equiv s/(uv) \pmod{\Lambda}$. To check this condition we have to create two tables containing the values $uv \bmod \Lambda$ and $s/(uv) \bmod \Lambda$ for any combination $(u, v) \in \mathcal{S} \times \mathcal{S}$. The most important limitation of this approach is that we will find Carmichael numbers with exactly $\kappa - 4$ factors only. Another disadvantage is the huge amount of memory required to store the tables.

After considering all these methods we decided to start from scratch and construct a set $\mathcal{T}$ by selecting $\mathcal{T} = \{u\}$ where $u \in \mathcal{S}$ and then successively adding suitable elements from $\mathcal{S}$ so that finally $\prod_{p \in \mathcal{T}} p \equiv s \pmod{\Lambda}$. In order to perform the necessary calculations modulo Λ, we use a set of moduli Q_j which are relatively prime in pairs to obtain a unique representation of the combinations of primes we will generate. The best we can do is to choose $Q_j = q_j^{h_j}$ for $j = 1, 2, \ldots, r$. Then $\Lambda = \prod_{j=1}^{r} Q_j$, and each possible prime factor p of the Carmichael number to be constructed has a unique representation modulo these Q_j. Now let $m_j(p)$ denote the value $p \bmod Q_j$. All necessary divisions by p modulo Λ can then be done using these numbers $m_j(p)$.

Our algorithm starts by generating a table of $m_j(p)$, $p \in \mathcal{S}$ and $j = 1, 2, \ldots, r$. Then we set $t \leftarrow s$ and, by successively dividing t by suitable primes $p \in \mathcal{S}$, we try to achieve $t = 1$. In the representation $t_j = t \bmod Q_j$, $j = 1, 2, \ldots, r$, this can be done by increasing the number of moduli with $t_j = 1$ in every stage μ of the algorithm. We do this by applying appropriate backtracking techniques on the table of the $m_j(p)$. For literature about such techniques see, e. g., [21, pp. 106–158]. To measure the progress of the algorithm, we define the function

$$\Omega(x) := \begin{cases} 0 & \text{if } x \bmod Q_j = 1 \text{ for } 1 \leq j \leq r, \\ \max_{\substack{1 \leq j \leq r \\ x \bmod Q_j \neq 1}} j & \text{otherwise} \end{cases}$$

for every natural number x. The values of the function $\Omega(x)$ become smaller the more remainders $x \bmod Q_j$ are 1 in sequence for decreasing j. Using this function, we demand $\Omega\left(t^{(\mu+1)}\right) < \Omega\left(t^{(\mu)}\right)$ for each stage μ in our algorithm.

Algorithm B

B1 [Initialize]. For every $p \in \mathcal{S}$, compute the remainders $m_j(p) \leftarrow p \bmod Q_j$, $j = 1, 2, \ldots r$. [For fixed j, the $m_j(p)$ can take $(q_j - 1)q_j^{h_j - 1}$ different values.] Initialize $\mu \leftarrow 1$, $\mathcal{T} \leftarrow \varnothing$, and $t^{(\mu)} \leftarrow s$.

B2 [Assign sets]. Set $\omega \leftarrow \Omega\left(t^{(\mu)}\right)$,

$$\mathcal{A}^{(\mu)} \leftarrow \left\{ u \;\middle|\; \begin{array}{l} u \in \mathcal{S} \smallsetminus \mathcal{T} \\ \wedge \; \Omega(u) = \omega \\ \wedge \; m_\omega(u) = t_\omega^{(\mu)} \end{array} \right\},$$

$$\mathcal{B}^{(\mu)} \leftarrow \left\{ (u,v) \;\middle|\; \begin{array}{l} u,v \in \mathcal{S} \smallsetminus \mathcal{T} \\ \wedge \; u < v \\ \wedge \; \Omega(u) = \Omega(v) = \omega \\ \wedge \; m_\omega(u)\, m_\omega(v) \equiv t_\omega^{(\mu)} \pmod{Q_\omega} \end{array} \right\},$$

$$\mathcal{C}^{(\mu)} \leftarrow \left\{ (u,v) \;\middle|\; \begin{array}{l} u,v \in \mathcal{S} \smallsetminus \mathcal{T} \\ \wedge \; u < v \\ \wedge \; \Omega(u) = \Omega(v) = \omega + 1 \\ \wedge \; m_{\omega+1}(u)\, m_{\omega+1}(v) \equiv 1 \pmod{Q_{\omega+1}} \\ \wedge \; m_\omega(u)\, m_\omega(v) \equiv t_\omega^{(\mu)} \pmod{Q_\omega} \end{array} \right\}.$$

B3 [Try element from $\mathcal{A}^{(\mu)}$]. If $\mathcal{A}^{(\mu)} \neq \varnothing$, select $u \in \mathcal{A}^{(\mu)}$, set $\mathcal{A}^{(\mu)} \leftarrow \mathcal{A}^{(\mu)} \smallsetminus \{u\}$, $\mathcal{Z}^{(\mu)} \leftarrow \{u\}$, $t^{(\mu+1)} \leftarrow t^{(\mu)}/u \bmod \Lambda$, and continue with step B7.

B4 [Try element from $\mathcal{B}^{(\mu)}$]. If $\mathcal{B}^{(\mu)} \neq \varnothing$, select $(u,v) \in \mathcal{B}^{(\mu)}$, set $\mathcal{B}^{(\mu)} \leftarrow \mathcal{B}^{(\mu)} \smallsetminus \{(u,v)\}$, $\mathcal{Z}^{(\mu)} \leftarrow \{u,v\}$, $t^{(\mu+1)} \leftarrow t^{(\mu)}/(uv) \bmod \Lambda$, and continue with step B7.

B5 [Try element from $\mathcal{C}^{(\mu)}$]. If $\mathcal{C}^{(\mu)} \neq \varnothing$, select $(u,v) \in \mathcal{C}^{(\mu)}$, set $\mathcal{C}^{(\mu)} \leftarrow \mathcal{C}^{(\mu)} \smallsetminus \{(u,v)\}$, $\mathcal{Z}^{(\mu)} \leftarrow \{u,v\}$, $t^{(\mu+1)} \leftarrow t^{(\mu)}/(uv) \bmod \Lambda$, and continue with step B7.

B6 [Backtrack]. Set $\mu \leftarrow \mu - 1$. If $\mu > 0$, set $\mathcal{T} \leftarrow \mathcal{T} \smallsetminus \mathcal{Z}^{(\mu)}$, $\omega \leftarrow \Omega\left(t^{(\mu)}\right)$, and continue with step B3, otherwise terminate the algorithm without finding a Carmichael number.

B7 [Set $\mathcal{T}$ found?]. Set $\mathcal{T} \leftarrow \mathcal{T} \cup \mathcal{Z}^{(\mu)}$. If $t^{(\mu+1)} \neq 1$, set $\mu \leftarrow \mu + 1$ and continue with step B2, otherwise we have found a suitable set $\mathcal{T}$.

Remarks. For the h_j considered in this paper, each $m_j(p)$ can be stored in a two-byte integer, and all $m_j(p)$ will fit in $2r\kappa$ bytes.

The sets $\mathcal{A}^{(\mu)}$, $\mathcal{B}^{(\mu)}$ and $\mathcal{C}^{(\mu)}$ do not require much calculation, since they represent sections of a sorted table of $p \in \mathcal{S}$. This sorting can be achieved during the generation of $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ in step C2. The remaining calculations for $\mathcal{B}^{(\mu)}$ and $\mathcal{C}^{(\mu)}$ can be deferred until they are first used in step B4 and B5, respectively.

When performing step B7, at most two primes are added to the set $\mathcal{T}$. In view of the fact that any occasional execution of step B6 removes the same number of primes as previously added by step B7, in the stage μ the set $\mathcal{T}$ contains at most 2μ primes. The assignments in step B2 ensure $\Omega\left(t^{(\mu+1)}\right) < \Omega\left(t^{(\mu)}\right)$. So, after at most $\mu = r$ stages we have $\Omega\left(t^{(\mu)}\right) = 0$, which is equivalent to $t^{(\mu)} = 1$. Therefore, the algorithm is able to find Carmichael numbers with a number of factors in the range from $\kappa - 2r$ up to κ.

All arithmetic modulo Λ can be done using the representation modulo Q_j. So we do not need to calculate $t^{(\mu)}$ but only $t_j^{(\mu)}$, $j = 1, \ldots, r$. The division $(t^{(\mu)}/p) \bmod \Lambda$ is then done by calculating $(t_j^{(\mu)}/m_j(p)) \bmod Q_j$, $j = 1, \ldots, r$. The actual value

$t^{(\mu)}$ can be generated from the values $t_j^{(\mu)}$ using the Chinese remainder theorem, but this is not necessary for the algorithm to work.

The selection of sets in step B2 can be justified by the following considerations. For a given stage μ the set $\mathcal{A}^{(\mu)}$ contains all primes $u \in \mathcal{S} \setminus \mathcal{T}$ which directly match with $t_\omega^{(\mu)}$. For ω large enough, the set $\mathcal{A}^{(\mu)}$ will not be empty and the algorithm can proceed with the next μ. However, for small ω in B2 we normally have $\mathcal{A}^{(\mu)} = \varnothing$ because there are much more possible remainders modulo Q_ω than primes with $\Omega(p) = \omega$. In this case we try to combine the required remainder from pairs (u, v) with $\Omega(u) = \Omega(v) = \omega$. All matching pairs are put into the set $\mathcal{B}^{(\mu)}$. Our experience has shown that in spite of all backtracking efforts these pairs are not always sufficient to find a suitable set $\mathcal{T}$. For this reason we have introduced the set $\mathcal{C}^{(\mu)}$, which contains matching pairs (u, v) with $\Omega(u) = \Omega(v) = \omega + 1$. We may consider taking additional sets $\mathcal{D}^{(\mu)}$, $\mathcal{E}^{(\mu)}$, ..., but we have not encountered any value of Λ for which the selection of sets given in step B2 failed to produce a Carmichael number.

In order to find more than one Carmichael number using the same set $\mathcal{S}$, we may record each $\mathcal{T}$ found in step B7, set $\mathcal{T} \leftarrow \mathcal{T} \setminus \mathcal{Z}^{(\mu)}$ and proceed with step B3. We can do this until we have found enough sets $\mathcal{T}$ or the algorithm terminates in step B6.

Example. We now return to our example from §2 where $\Lambda = 5040$. In step C2 we build the numbers $p(\alpha_1, \alpha_2, \ldots, \alpha_r)$ by performing r nested loops on the α_j where the index α_1 varies most rapidly. In this way, step C3 implicitly generates a table of all p sorted according to $\Omega(p)$ in descending order.

Step B1. We compute the remainders $m_j(p) \leftarrow p \bmod Q_j, j = 1, 2, 3, 4$, and the values of $\Omega(p)$ as follows:

p	$p \bmod 2^4$	$p \bmod 3^2$	$p \bmod 5$	$p \bmod 7$	$\Omega(p)$
17	1	8	2	3	4
13	13	4	3	6	4
19	3	1	4	5	4
37	5	1	2	2	4
73	9	1	3	3	4
11	11	2	1	4	4
41	9	5	1	6	4
31	15	4	1	3	4
61	13	7	1	5	4
241	1	7	1	3	4
181	5	1	1	6	4
29	13	2	4	1	3
113	1	5	3	1	3
43	11	7	3	1	3
337	1	4	2	1	3
127	15	1	2	1	3
1009	1	1	4	1	3
71	7	8	1	1	2
281	9	2	1	1	2
211	3	4	1	1	2
421	5	7	1	1	2
631	7	1	1	1	1
2521	9	1	1	1	1

We initialize $\mu \leftarrow 1$, $\mathcal{T} \leftarrow \varnothing$, and
$t_1^{(1)} \leftarrow 1$, $t_2^{(1)} \leftarrow 2$, $t_3^{(1)} \leftarrow 4$, $t_4^{(1)} \leftarrow 5$, calculated from $s = 929$.

Step B2. We set $\omega \leftarrow 4$,
$\mathcal{A}^{(1)} \leftarrow \{19, 61\}$,
$\mathcal{B}^{(1)} \leftarrow \{(11, 17), (11, 31), (11, 37), (11, 73), (11, 241), (13, 37), (37, 181)\}$,
$\mathcal{C}^{(1)} \leftarrow \varnothing$.

Step B3. $\mathcal{A}^{(1)} = \{19, 61\} \neq \varnothing$,
therefore we select $u = 19$ and we set $\mathcal{A}^{(1)} \leftarrow \{61\}$,
$\mathcal{Z}^{(1)} \leftarrow \{19\}$, $t_1^{(2)} \leftarrow 11$, $t_2^{(2)} \leftarrow 2$, $t_3^{(2)} \leftarrow 1$, $t_4^{(2)} \leftarrow 1$.

Step B7. $\mathcal{T} \leftarrow \{19\}$, $t^{(2)} \neq 1$, $\mu \leftarrow 2$.

Step B2. We set $\omega \leftarrow 2$,
$\mathcal{A}^{(2)} \leftarrow \{281\}$,
$\mathcal{B}^{(2)} \leftarrow \{(71, 421)\}$,
$\mathcal{C}^{(2)} \leftarrow \{(29, 1009), (113, 337)\}$.

Step B3. $\mathcal{A}^{(2)} = \{281\} \neq \varnothing$,
therefore we select $u = 281$ and we set $\mathcal{A}^{(2)} \leftarrow \varnothing$,
$\mathcal{Z}^{(2)} \leftarrow \{281\}$, $t_1^{(3)} \leftarrow 3$, $t_2^{(3)} \leftarrow 1$, $t_3^{(3)} \leftarrow 1$, $t_4^{(3)} \leftarrow 1$.

Step B7. $\mathcal{T} \leftarrow \{19, 281\}$, $t^{(3)} \neq 1$, $\mu \leftarrow 3$.

Step B2. We set $\omega \leftarrow 1$, $\mathcal{A}^{(3)} \leftarrow \varnothing$, $\mathcal{B}^{(3)} \leftarrow \varnothing$, $\mathcal{C}^{(3)} \leftarrow \varnothing$, all sets are empty.

Step B6. We set $\mu \leftarrow 2$.
[Now are active
$\mathcal{A}^{(2)} = \varnothing$, $\mathcal{B}^{(2)} = \{(71, 421)\}$, $\mathcal{C}^{(2)} = \{(29, 1009), (113, 337)\}$,
$\mathcal{Z}^{(2)} = \{281\}$, $t_1^{(2)} = 11$, $t_2^{(2)} = 2$, $t_3^{(2)} = 1$, $t_4^{(2)} = 1$.]
We set $\mathcal{T} \leftarrow \{19\}$, $\omega \leftarrow 2$.

Step B4. $\mathcal{B}^{(2)} = \{(71, 421)\} \neq \varnothing$,
therefore we select $(u, v) = (71, 421)$ and we set $\mathcal{B}^{(2)} \leftarrow \varnothing$,
$\mathcal{Z}^{(2)} \leftarrow \{71, 421\}$, $t_1^{(3)} \leftarrow 9$, $t_2^{(3)} \leftarrow 1$, $t_3^{(3)} \leftarrow 1$, $t_4^{(3)} \leftarrow 1$.

Step B7. $\mathcal{T} \leftarrow \{19, 71, 421\}$, $t^{(3)} \neq 1$, $\mu \leftarrow 3$.

Step B2. We set $\omega \leftarrow 1$, $\mathcal{A}^{(3)} \leftarrow \{2521\}$, $\mathcal{B}^{(3)} \leftarrow \varnothing$, $\mathcal{C}^{(3)} \leftarrow \varnothing$.

Step B3. $\mathcal{A}^{(3)} = \{2521\} \neq \varnothing$,
therefore we select $u = 2521$ and we set $\mathcal{A}^{(3)} \leftarrow \varnothing$,
$\mathcal{Z}^{(3)} \leftarrow \{2521\}$, $t_1^{(4)} \leftarrow 1$, $t_2^{(4)} \leftarrow 1$, $t_3^{(4)} \leftarrow 1$, $t_4^{(4)} \leftarrow 1$.

Step B7. $\mathcal{T} \leftarrow \{19, 71, 421, 2521\}$, and we have $t^{(4)} = 1$.

With (5) we find $N = \prod_{p \in \mathcal{S} \setminus \mathcal{T}} p = 11 \cdot 13 \cdot 17 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 73 \cdot 113 \cdot 127 \cdot 181 \cdot 211 \cdot 241 \cdot 281 \cdot 337 \cdot 631 \cdot 1009$, a Carmichael number with 19 factors.

Continuing the search, we find more sets $\mathcal{T} = \{19, 29, 631, 1009\}$, $\{61, 211, 281, 631, 1009, 2521\}$, $\{43, 61, 113, 631, 2521\}$, $\{43, 61, 113, 211, 421\}$, $\{61, 71, 127, 337, 421, 2521\}$, $\{29, 61, 127, 337, 631, 1009\}$, $\{19, 31, 61, 281\}$, $\{19, 31, 61, 113, 337, 2521\}$, $\{19, 61, 113, 127, 241, 2521\}$, yielding Carmichael numbers with 19, 17, 18, 18, 17, 17, 19, 17, 17 factors respectively.

4. COMPUTATIONAL RESULTS

In this section we present some of the Carmichael numbers we found during our research. Because of the size of most of these numbers, we do not include all their factors, but only Λ, k, and $\mathcal{T}$. In addition we supply the number d of decimal digits for each N listed. Unfortunately, this form of presentation leaves it to the reader to recompute the whole set $\mathcal{S}$ if he wants to get hold of all the factors.

TABLE 1. A Carmichael number for every k,
$21 \leq k \leq 100$ characterized by Λ, d, and $\mathcal{T}$

k	Λ	d	$\mathcal{T}$	k	Λ	d	$\mathcal{T}$
21	19800	47	$\{31, 199, 397, 9901\}$	61	739200	186	$\{13, 29, 3851, 5281\}$
22	12600	52	$\{11, 13, 71, 281\}$	62	1524600	196	$\{61, 73, 211\}$
23	10080	52	$\{13, 19, 29, 211\}$	63	332640	184	$\{13, 113, 211, 991\}$
24	10080	53	$\{31, 71, 73\}$	64	2744280	198	$\{109, 2377, 25411\}$
25	23760	58	$\{19, 23, 37\}$	65	846720	199	$\{13, 421, 2521\}$
26	28080	60	$\{19, 181\}$	66	5556600	220	$\{11, 29, 24697, 370441\}$
27	27720	64	$\{13, 89, 331, 463\}$	67	604800	195	$\{401, 2161, 21601\}$
28	27720	65	$\{41, 421, 661\}$	68	554400	199	$\{41, 97, 110881\}$
29	32760	74	$\{11, 37, 43, 547\}$	69	1247400	212	$\{29, 109, 331, 7129\}$
30	32760	72	$\{29, 1093, 8191\}$	70	1411200	220	$\{17, 71, 577, 1801\}$
31	25200	78	$\{11, 13, 31, 73\}$	71	720720	218	$\{17, 71, 331, 4621\}$
32	25200	77	$\{11, 19, 4201\}$	72	1587600	221	$\{29, 757, 176401\}$
33	30240	79	$\{11, 43, 2161\}$	73	1386000	224	$\{881, 4201, 18481\}$
34	42840	87	$\{31, 281\}$	74	1921920	233	$\{29, 2003, 960961\}$
35	376320	99	$\{13, 1471, 5881, 17921\}$	75	5670000	249	$\{11, 41, 43, 337\}$
36	1778700	110	$\{3301, 3631, 11551, 12101\}$	76	17287200	266	$\{211, 2801, 54881\}$
37	823200	107	$\{13, 17, 101, 137201\}$	77	997920	237	$\{17, 199, 433, 23761\}$
38	508200	111	$\{211, 15401, 84701\}$	78	997920	238	$\{617, 673, 4159\}$
39	141120	102	$\{11, 181, 2017, 7841\}$	79	2268000	248	$\{3001, 4001\}$
40	161280	109	$\{11, 37, 71, 26881\}$	80	4851000	264	$\{3001, 19801, 231001\}$
41	161280	107	$\{673, 2689, 20161\}$	81	3528000	271	$\{11, 31, 2017, 3361\}$
42	90720	107	$\{113, 2017, 7561\}$	82	2522520	274	$\{29, 547, 126127\}$
43	90720	110	$\{41, 6481\}$	83	3175200	268	$\{11, 281, 1051, 21601\}$
44	470400	125	$\{17, 337, 78401\}$	84	1330560	260	$\{17, 61, 4481, 8317\}$
45	138600	120	$\{601, 15401, 19801\}$	85	2116800	273	$\{337, 5881, 211681\}$
46	1190700	140	$\{71, 883, 1051\}$	86	25930800	308	$\{19, 2161, 21169, 5186161\}$
47	873180	135	$\{67, 6469, 32341\}$	87	4762800	290	$\{487, 2801, 158761\}$
48	151200	127	$\{13, 101\}$	88	1995840	275	$\{43, 661, 45361\}$
49	241920	133	$\{11, 379, 577\}$	89	1441440	282	$\{89, 241, 18481\}$
50	1358280	150	$\{71, 991, 271657\}$	90	12492480	318	$\{31, 8009, 35491\}$
51	221760	138	$\{13, 181, 1321, 2521\}$	91	8537760	321	$\{19, 73, 3361, 32341\}$
52	166320	143	$\{19, 61, 127\}$	92	8537760	322	$\{211, 421, 142297\}$
53	3150000	170	$\{13, 43, 1051, 126001\}$	93	26486460	343	$\{67, 859, 8581, 25741\}$
54	1323000	162	$\{13, 541, 12601\}$	94	4158000	309	$\{29, 397, 601, 1051\}$
55	2845920	183	$\{13, 241, 463, 3631\}$	95	2217600	307	$\{73, 1409, 4481\}$
56	403200	162	$\{61, 127, 211\}$	96	3880800	324	$\{19, 661, 1321, 9901\}$
57	360360	168	$\{73, 89, 9241\}$	97	8408400	346	$\{53, 211, 1301, 2861\}$
58	529200	169	$\{11, 631, 6301\}$	98	8408400	344	$\{463, 4201, 1401401\}$
59	5880000	192	$\{7351, 12251, 735001\}$	99	7927920	343	$\{19, 331, 463, 76231\}$
60	7507500	211	$\{61, 26251, 50051\}$	100	7927920	346	$\{113, 241, 8009\}$

We started our work in 1987 on an AT-compatible PC running DOS 3.1 and tried to find an example of a Carmichael number with k prime factors for every k below a given limit. We obtained Carmichael numbers for every $k \leq 134$ [13]. For $k \leq 20$, Pinch [16] has created a table of the smallest Carmichael number with k factors. An example for every k, $21 \leq k \leq 100$, is shown in Table 1.

In order to find larger Carmichael numbers, we switched from the PC to a Siemens 7·882 mainframe and soon found a number with 344 factors, published in 1988 [13]. With a slightly improved program we found numbers with up to 3316 factors. Some intermediate results are shown in Table 2.

TABLE 2. Some Carmichael numbers
found using our previous algorithms

Λ	k	d	$\mathcal{T}$
931170240	344	1536	$\{419, 1171, 2081, 29173\}$
931170240	344	1531	$\{43, 7393, 2217073, 2238391\}$
97772875200	1034	5654	$\{1471, 257401, 471241, 9831361\}$
97772875200	1034	5656	$\{4561, 8191, 287281, 383041\}$
97772875200	1034	5653	$\{12601, 93601, 270271, 7261801\}$
3855044793600	2017	12511	$\{163, 12541, 14081, 532097281\}$
74530866009600	3312	22722	$\{449, 10337, 162691, 5986993\}$

TABLE 3. Some medium-sized Carmichael
numbers calculated on an IBM PS/2-70 PC

$\Lambda = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 931170240$
$k = 340$, $K(\Lambda) = 361$, $N = 11858668\ldots98349441$, $d = 1504$, Time $= 30\,\mathrm{s}$

$\mathcal{T} = \{$	67,	302329,	1108537,	3233231,	232792561,	
	72353,	1058149,	2771341			$\}$

$\Lambda = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 97772875200$
$k = 1029$, $K(\Lambda) = 1009$, $N = 56150711\ldots42742401$, $d = 5611$, Time $= 2\,\mathrm{m}\ 57\,\mathrm{s}$

$\mathcal{T} = \{$	97,	75583,	362121761,	905304401,	24443218801,	
	7753,	1108537,	665121601,	10863652801		$\}$

$\Lambda = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 3855044793600$
$k = 2009$, $K(\Lambda) = 2005$, $N = 19624530\ldots79955201$, $d = 12429$, Time $= 9\,\mathrm{m}\ 7\,\mathrm{s}$

$\mathcal{T} = \{$	23599,	11531521,	2677114441,	16062686641,	26771144401,	
	29717,	478056151,	13385572201,	20078358301,	40156716601,	
	2897311,	637408201				$\}$

$\Lambda = 2^9 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = 74530866009600$
$k = 3305$, $K(\Lambda) = 3245$, $N = 12973148\ldots50790401$, $d = 22647$, Time $= 18\,\mathrm{m}\ 49\,\mathrm{s}$

$\mathcal{T} = \{$	37,	27373681,	1680439801,	20703018337,	232908956281,	
	300151,	1433975297,	5041319401,	86262576401,	1035150916801,	
	15511753					$\}$

$\Lambda = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 = 24259796886124800$
$k = 10058$, $K(\Lambda) = 9895$, $N = 24661064\ldots20019201$, $d = 81488$, Time $= 89\,\mathrm{m}\ 57\,\mathrm{s}$

$\mathcal{T} = \{$	15534721,	937908721,	2200435091713,	189529663172851,	1155228423148801,	
	125349841,	28130562253,	84235405854601,	1010824870255201,	6064949221531201,	
	320576209,	1069655947361,	138627410777857			$\}$

In 1989 we switched back from the mainframe to an IBM PS/2-70 PC, running OS/2 to overcome space limitations. After developing algorithm B we found Carmichael numbers with up to $k = 10058$ factors [15], some of which are presented in Table 3. For each of these numbers, the values of Λ, k, and the set $\mathcal{T}$ are given. Furthermore, we list the expected size of the set $\mathcal{S}$ as predicted by our function $K(\Lambda)$, the first eight and the last eight digits of N, the total number of digits d of N, and the time used to find N on an IBM PS/2-70 personal computer. The actual size κ of the set $\mathcal{S}$ used for each of these calculations is given by $\kappa = k + \#\mathcal{T}$.

The next challenge now was to find a Carmichael number with more than one

TABLE 4. Some of the largest Carmichael numbers
found on an IBM RS/6000-550 workstation

$\Lambda = 2^{10} \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 = 94949448640728409728000$

$k = 125504$, $K(\Lambda) = 122685$, $N = 11902822\ldots15488001$, $d = 1424198$, Time $= 36$ m

$\mathcal{T} = \{$

1599361,	31350370847401,	6593711711161695121,
24371713,	39209074920091,	6868449699126765751,
23295294721,	2174796688900993,	80739327075449328001,
82848588481,	164842792779042379,	1483585135011381402001,
1383849703063,	3391051737168871777,	5274969368929356096001,
6555077540821		}

$\Lambda = 2^{11} \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 = 104444393504801250070080000$

$k = 244767$, $K(\Lambda) = 239874$, $N = 41121806\ldots48640001$, $d = 3025356$, Time $= 1$ h 24 m

$\mathcal{T} = \{$

391387,	67962396528157,	198941701913907144193,
1681557571,	11808850799462401,	335790874179530770001,
11259392449,	1918804995311604401,	906635360284733079001,
23295294721,	15110589338078884651,	21490615947489969280001,
1011586040251,	83947718544882692501,	24176942940926215440001,
17426255520041,	195731702001089280001	}

$\Lambda = 2^{14} \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 = 977599952320493970655594880000$

$k = 577424$, $K(\Lambda) = 566982$, $N = 50355100\ldots38080001$, $d = 7976462$, Time $= 4$ h 10 m

$\mathcal{T} = \{$

42901,	1678099850964179921,	384857459059641179680001,
52642897921,	3975800196897127,	43887745149492242718721,
60868350721,	35570472767505649,	397786264324926638411251,
188691887233,	16035727460818408201,	127291604583976524291600001,
1383849703063,	9429007746961224021601,	1508641239513795843456000001,
1801502791681,	1309584409300170003000001,	24138259832220733495296001 }

$\Lambda = 2^{14} \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 = 166191918944839750115112960000$

$k = 838670$, $K(\Lambda) = 823789$, $N = 10124726\ldots66240001$, $d = 12096430$, Time $= 6$ h 40 m

$\mathcal{T} = \{$

54765569,	2654367240812492801,	100183207311463005229501,
582382369,	3028970742599032661,	2051752085738762347100161,
33398272001,	43797414969018740017,	210775059538402686327000001,
3933046524493,	1484195663873526003400001,	384703516076017940081280001,
1691371859298001,	6440349041451193193325 1	}

$\Lambda = 2^{14} \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 = 4594717759063216620829593600000$

$k = 1101518$, $K(\Lambda) = 1082068$, $N = 70388830\ldots50240001$, $d = 16142049$, Time $= 9$ h 18 m

$\mathcal{T} = \{$

3747815171101,	373725218508329844001,	5627471290249873384320 1,
7937871675841,	527575433460925629781,	1025841120618466502350 01,
157662554664961,	100490558754462024720 1,	1594560932302207334400 01,
7166547582616451,	1500659010733299569153,	830931307700957866903500 1,
14386014397937074177,	25646028015461662558751,	4254368295428904278545920001 }

---

million factors. We ported our program to an IBM RS/6000-550 workstation and finally discovered a Carmichael number with 1101518 factors. Five Carmichael numbers with more than 100000 factors can be found in Table 4. The computing times given in this table refer to an IBM RS/6000-550 workstation. This workstation is about 80 times faster than the PC we used before. On this PC, the first Carmichael number from Table 4 with $k = 125504$ factors needed 46 hours and 33 minutes. In any case, it should be noted that the steps C2 and C3 consume about 98% of the listed time while the subsequent step C4 as performed using algorithm B produces the Carmichael numbers very quickly.

TABLE 5. Progress in discovering large Carmichael numbers

Carmichael number N		k	d	Year	Discoverer
$7 \cdot 31 \cdot 73$	15841	3	5	1910	Carmichael
$13 \cdot 37 \cdot 73 \cdot 457$	16046641	4	8	1912	Carmichael
$5 \cdot 97 \cdot 109 \cdot 1889$	99861985	4	8	1938	Poulet
$5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673 \cdot 2689$	169875651141505	7	15	1939	Chernick
$11 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 79 \cdot 97 \cdot 113 \cdot 127 \cdot 131 \cdot 151$					
	4436563378934455936090566001	15	27	1978	Yorinaga
	57736720 ... 48486881	3	77	1979	Hill
	51009765 ... 51976601	3	321	1980	Wagstaff
	80194635 ... 30286001	4	432	1982	Woods, Huenemann
	43407186 ... 00000001	3	1057	1985	Dubner
	14276304 ... 03279041	344	1536	1988	Löh
	12831493 ... 66519553	3	3710	1988	Dubner
	24661064 ... 20019201	10058	81488	1989	Löh, Niebuhr
	70388830 ... 50240001	1101518	16142049	1992	Löh, Niebuhr

For all Carmichael numbers found by our programs, the conditions $\prod_{p \in \mathcal{T}} p \equiv s$ (mod Λ) and $\prod_{p \in \mathcal{S} \setminus \mathcal{T}} p \equiv 1$ (mod Λ) have been individually checked.

Table 5 shows the world-wide progress in the search for large Carmichael numbers N. For the first five entries, the table contains the complete factorization of N together with their full decimal notation. For the later entries, we list only the first eight and the last eight digits of N.

By the way, applying (4) on

$$\Lambda = 2^{15} \cdot 3^8 \cdot 5^5 \cdot 7^4 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79,$$

we get $K(\Lambda) = 1009441849$. Therefore, if this Λ were used as input, we would expect Carmichael numbers to appear with about one billion factors. This expectation is in good accord with the fact that Alford, Granville and Pomerance have proved the existence of infinitely many Carmichael numbers [1].

REFERENCES

1. W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), 703–722. CMP 94:15
2. N. G. W. H. Beeger, *On composite numbers n for which $a^{n-1} \equiv 1$ (mod n) for every a prime to n*, Scripta Math. **16** (1950), 133–135. MR **12**:159e
3. R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232–238.
4. _____, *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1$ (mod P)*, Amer. Math. Monthly **19** (1912), 22–27.
5. J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), 269–274.
6. H. Dubner, *A new method for producing large Carmichael numbers*, Math. Comp. **53** (1989), 411–414. MR **89m**:11013
7. P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), 201–206. MR **18**:18e
8. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, Addison-Wesley, Reading, MA, 1989. MR **91f**:00001
9. D. Guillaume and F. Morain, *Building Carmichael numbers with a large number of prime factors and generalization to other numbers*, preprint, June 1992.

10. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Clarendon Press, Oxford, 1979. MR **81i:**10002
11. J. R. Hill, *Large Carmichael numbers with three prime factors*, Notices Amer. Math. Soc. **26** (1979), #79T–A–136.
12. D. E. Knuth, *The art of computer programming,* Vol. 2, 2nd ed., Addison-Wesley, Reading, MA, 1980. MR **83i:**68003
13. G. Löh, *Carmichael numbers with a large number of prime factors*, Abstracts Amer. Math. Soc. **9** (1988), 329.
14. _____, *Long chains of nearly doubled primes*, Math. Comp. **53** (1989), 751–759. MR **90e:**11015
15. G. Löh and W. Niebuhr, *Carmichael numbers with a large number of prime factors,* II, Abstracts Amer. Math. Soc. **10** (1989), 305.
16. R. G. E. Pinch, *The Carmichael numbers up to 10^{15}*, Math. Comp. **61** (1993), 381–391. MR **93m:**11137
17. _____, *Some primality testing algorithms*, Notices Amer. Math. Soc. **40** (1993), 1203–1210.
18. P. Poulet, *Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à* 100.000.000, Sphinx **8** (1938), 42–52; Corrections: MTE 485, Math. Comp. **25** (1971), 944–945; MTE 497, Math. Comp. **26** (1972), 814.
19. P. A. Pritchard, A. Moran, and A. Thyssen, *Twenty-two primes in arithmetic progression*, Math. Comp. **64** (1995), 1337–1339.
20. S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. (2) **14** (1915), 347–409.
21. E. M. Reingold, J. Nievergelt, and N. Deo, *Combinatorial algorithms*, Prentice-Hall, Englewood Cliffs, NJ, 1977. MR **57:**11164
22. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Boston, MA, 1985. MR **88k:**11002
23. S. S. Wagstaff, Jr., *Large Carmichael numbers*, Math. J. Okayama Univ. **22** (1980), 33–41. MR **82c:**10007
24. D. Woods and J. Huenemann, *Larger Carmichael numbers*, Comput. Math. Appl. **8** (1982), 215–216. MR **83f:**10017
25. M. Yorinaga, *Numerical computation of Carmichael numbers*, Math. J. Okayama Univ. **20** (1978), 151–163. MR **80d:**10026
26. _____, *Carmichael numbers with many prime factors*, Math. J. Okayama Univ. **22** (1980), 169–184. MR **81m:**10018
27. M. Zhang, *Searching for large Carmichael numbers*, Sichuan Daxue Xuebao **29** (1992), 472–474, (Chinese, abridged version in English).

REGIONALES RECHENZENTRUM DER UNIVERSITÄT HAMBURG, SCHLÜTERSTRASSE 70, 20146 HAMBURG, GERMANY
E-mail address: `rz2a011@rrz.uni-hamburg.de`

REGIONALES RECHENZENTRUM DER UNIVERSITÄT HAMBURG, SCHLÜTERSTRASSE 70, 20146 HAMBURG, GERMANY
Current address: Lisztstraße 6b, 22763 Hamburg, Germany
E-mail address: `100117.256@compuserve.com`